REC'D 13 JUN 2005
WIPO PCT

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference PU030081	FOR FURTHER ACTION	See Form PCT/IPEA/416
International application No. PCT/US04/07403	International filing date *(day/month/year)* 11 March 2004 (11.03.2004)	Priority date *(day/month/year)* 14 March 2003 (14.03.2003)
International Patent Classification (IPC) or national classification and IPC IPC(7): H04H 1/00; H04L 9/00 and US Cl.: 370/312; 713/172, 183		
Applicant THOMSON LICENSING S.A.		

1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 3 sheets, including this cover sheet.
3. This report is also accompanied by ANNEXES, comprising:

   a. ☒ *(sent to the applicant and to the International Bureau)* a total of 11 sheets, as follows:

      □ sheets of the description, claims and/or drawings which have been amended and are the basis of this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).

      □ sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.

   b. □ *(sent to the International Bureau only)* a total of (indicate type and number of electronic carrier(s))

      _____ , containing a sequence listing and/or tables related thereto, in computer readable form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).

4. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
□	Box No. II	Priority
□	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
□	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
□	Box No. VI	Certain documents cited
□	Box No. VII	Certain defects in the international application
□	Box No. VIII	Certain observations on the international application

Date of submission of the demand 08 December 2004 (08.12.2004)	Date of completion of this report 31 May 2005 (31.05.2005)
Name and mailing address of the IPEA/ US Mail Stop PCT, Attn: IPEA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703) 305-3230	Authorized officer Ayaz Sheikh Telephone No. 571-272-3000

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/US04/07403

Box No. I Basis of the report

1. With regard to the **language**, this report is based on the international application in the language in which it was filed, unless otherwise indicated under this item.

   □ This report is based on translations from the original language into the following language __________ , which is the language of a translation furnished for the purposes of:

   □ international search (under Rules 12.3 and 23.1(b))
   □ publication of the international application (under Rule 12.4)
   □ international preliminary examination (under Rules 55.2 and/or 55.3)

2. With regard to the **elements** of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report)*:

   □ the international application as originally filed/furnished

   ☒ the description:
   pages 1-5 & 7 as originally filed/furnished
   pages* 6,8 and 9 received by this Authority on 08 December 2004 (08.12.2004)
   pages* NONE received by this Authority on __________

   ☒ the claims:
   pages __________ as originally filed/furnished
   pages* NONE as amended (together with any statement) under Article 19
   pages* 10-14 received by this Authority on 08 December 2004 (08.12.2004)
   pages* NONE received by this Authority on __________

   ☒ the drawings:
   pages NONE as originally filed/furnished
   pages* 1-3 received by this Authority on 08 December 2004 (08.12.2004)
   pages* NONE received by this Authority on __________

   □ a sequence listing and/or any related table(s) - see Supplemental Box Relating to Sequence Listing.

3. □ The amendments have resulted in the cancellation of:

   □ the description, pages__________
   □ the claims, Nos__________
   □ the drawings, sheets/figs__________
   □ the sequence listing (*specify*):__________
   □ any table(s) related to the sequence listing (*specify*):__________

4. □ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

   □ the description, pages__________
   □ the claims, Nos__________
   □ the drawings, sheets/figs__________
   □ the sequence listing (*specify*):__________
   □ any table(s) related to the sequence listing (*specify*):__________

* *If item 4 applies, some or all of those sheets may be marked "superseded."*

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/US04/07403

Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims 1-24	YES
	Claims NONE	NO
Inventive Step (IS)	Claims 1-24	YES
	Claims NONE	NO
Industrial Applicability (IA)	Claims 1-24	YES
	Claims NONE	NO

2. Citations and Explanations (Rule 70.7)

Claims 1-24 meet the criteria set out in PCT Article 33(2)-(3), because the prior art does not teach or fairly suggest providing secure communication session with a mobile terminal in a WLAN environment with a periodic key update and a secure log off, thus prior art does not provide a method where once the user is authenticated and the session key is established, future key updates are no longer required the participation of the authentication server because encrypted key update or log off request that is additionally encrypted with a session key.

------------------ NEW CITATIONS ------------------

terminal such as a laptop) may participate in the authentication of one or more wireless mobile devices $140_{1-n,}$, a local or back end server 120 and an authentication server 150.

In accordance with the present principles, the access 160 enables each mobile terminals $140_{1-n,}$ to securely access the WLAN 115 by authenticating both the mobile terminal itself, as well as its communication stream in accordance with the IEEE 802.1x protocol. The manner in which the access 160 enables such secure access can best be understood by reference to FIG. 1 in conjunction with FIG. 2.

The sequence of interactions that occurs over time among a mobile wireless communication device, say mobile terminal $140_{n,}$ the public WLAN 115, the local web server 120, and the authentication server 150 is described under the convention of an IEEE 802.1x protocol, wherein the access point 130_n of FIG. 1 maintains a controlled port and an un-controlled port, through which the access point exchanges information, with the mobile terminals 140_{1-n}. The controlled port maintained by the access point 130_n serves as the entryway for non-authentication information, such as data traffic to pass through the access point 130_n as it flows between the local server 120 and the mobile terminals 140_{1-n}. Ordinarily, the access points 130_{1-n} keep the respective controlled port closed in accordance with the IEEE 802.1x protocol, until the authentication of the pertinent mobile terminal 140_{1-n} communicates. The access points 130_{1-n} always maintain the respective uncontrolled port open to permit the mobile terminals 140_{1-n} to exchange authentication data with an authentication server 150.

More specifically, with reference to FIG. 2, a method in accordance with the present invention for improving the security of a mobile terminal in 140_n in a WLAN environment installs two shared secrets instead of one shared secret, on both the mobile terminal 140_n and the WLAN access point 130_n during the user authentication phase. One of the shared secrets is used as the initial session key and the other is used as a secure seed. Since the initial authentication is secure, these two keys would not be known to a would be hacker. The keys may be generated and distributed to the mobile terminal and the WLAN, access point, using known methods, for example using an authentication server, for generating and distributing such keys. Although the initial session key may eventually be cracked by the would be hacker, the secure seed remains secure as it is not used in any unsecure communication. More

IPEA/US

invokes via an ActiveX command of an ActiveX control though the device browser software. The ActiveX control is essentially an executable program that can be embedded inside a web page. Many software browser programs, such Microsoft Internet Explorer have the capability of displaying such web pages and invoking the embedded ActiveX controls, which can be downloaded from a remote server (e.g., the authentication server 150). The execution of the ActiveX controls are restricted by the security mechanisms built into the browser software. In practice, most browser programs have several different selectable security levels. At the lowest level, any ActiveX control from the web can be invoked without restriction. In the highest level, no ActiveX control can be invoked from the browser software.

A method in accordance with the present invention comprises the step of, after authentication and authorization, generating a first key in step 217 and distributing the new key to the access point 130_n and the mobile terminal 140_n. In step 121 second key referenced to as secure seed 123 is distributed to the mobile terminal 140_n and the access point 130_n. Thereafter the mobile terminal and the access point communicate using the first key as the session to encrypt the data. Thereafter, the access point 130_n and the mobile terminal 140_n employ the key 119 and the secure seed 123 to periodically generate 225a new session key 121, whereby the new session key is then used for subsequent communications between the mobile terminal and the access point. The second key is always stored and kept as a secret in the mobile terminal and the access point during the communication session so that a would be hacker is unable to determine the second key. Several techniques may be employed to further facilitate the management of the combined keys such as generating the new session key and concatenating the new session key to the secure seed prior to using it for security. Once having concatenated the combined session key and secure seed, the process may calculate a hash algorithm on the concatenated new session key and secure seed and generate a fixed string for further transmission.

A method for improving the security of a mobile terminal in a WLAN environment further comprises the steps of the mobile terminal 140_n sending during session logoff an encrypted logoff request accompanied by the secure seed such that the secure seed appears in the logoff request. As depicted in Fig. 3, during session logoff the mobile terminal 140_n remains secure to prevent a would be hacker from logging off an authenticated mobile terminal 140_n. The IEEE 802.1x based scheme cannot provide secure logoff because the logoff request is carried in an unencrypted frame. However in an embodiment of the present invention the mobile terminal 140_n sends an encrypted logoff request 228 accompanied by the secure seed 123. Thus even in the case where the would be hacker cracks the session key, log off of the authenticated user on mobile terminal 140_n would not be possible, since the secure seed 123 appears in the logoff request 228 and is no longer used since a new secure seed needs to be negotiated each time the user logs in.

In FIG. 4, is shown an apparatus for a secure communications session between the mobile terminal 140_n and WLAN. The access point 130_n comprises a means for generating a first and second secure key 410 and a means for transmitting 420 the first secure key 119 and the second secure key 123 to the mobile terminal 140_n. The mobile terminal 140_n receives the first secure key 119 and second secure key 123 and stores the keys in a register 430 for use during the secure communications session. The access point 130_n includes a means to encrypt 415 data and a means to transmit 420 data to the mobile terminal 140_n via the WLAN 115 using a current session key. The mobile terminal 140_n, includes a means to receive 450 and a means to decrypt data 435 received from the access point 130_n using the current session key 119, the first secure key initially being used as the current session key 119. The access point 130_n includes a means to periodically generate 425 a subsequent session key using the second secure key and using the subsequent session key as the current session key during subsequent communications between the WLAN 115 and the mobile terminal 140_n.

It is to be understood that the form of this invention as shown is merely a preferred embodiment. Various changes may be made in the function and arrangement of parts; equivalent means may be substituted for those illustrated and described; and certain features may be used independently from others without departing from the spirit and scope of the invention as defined in the following claims.

IPEA/US

PCT/US04/07403 .08122004

We Claim:

1. A method for providing a secure communications session with a user terminal in a communications network, the method comprising the steps of:

transmitting a secure key and a secure seed to the user terminal using a secure communications method, the secure key and the secure seed being suitable for storage in the user terminal for use during the secure communications session;

encrypting and transmitting data to the user terminal using a current session key, and receiving and decrypting data received from the user terminal using the current session key, the secure key initially being used as the current session key; and

periodically generating by an access point (AP) a subsequent session key using the secure seed and using the subsequent session key as the current session key during subsequent communications between the communications network and the user terminal.

2. The method according to claim 1, further comprising the step of:

logging off the user terminal in response to an encrypted logoff request from the user terminal accompanied by the secure seed.

3. The method according to claim 1, wherein the periodically generating step comprises generating the subsequent session key by concatenating the current session key with the secure seed and applying a hash algorithm.

4. A method for providing a secure communications session with a mobile terminal in a wireless local area network (WLAN), the method comprising the steps of:

transmitting a secure key and a secure seed to the mobile terminal using a secure communications method, the secure key and the secure seed being suitable for storage in the mobile terminal for use during the secure communications session;

encrypting and transmitting data to the mobile terminal using a current session key, and receiving and decrypting data received from the mobile terminal using the current session key, the secure key initially being used as the current session key; and

periodically generating by an access point (AP) a subsequent session key using the secure seed and using the subsequent session key as the current session key during subsequent communications with the mobile terminal.

AMENDED SHEET

IPEA/US

PCT/US04/07403 .08122004

5. The method as in claim 4, wherein the periodically generating step comprises generating by the AP a subsequent session key using a combination of a new key and the secure seed, the new key being generated using the secure key.

6. The method as in claim 5, wherein the periodically generating step comprises generating by the AP a subsequent session key by concatenating the new key and the secure seed and running a hash algorithm to generate the subsequent session key.

7. A method for providing a secure communications session with a mobile terminal in a wireless local area network (WLAN), the method comprising the steps of:

generating a secure key;

transmitting the secure key to the mobile terminal using a secure communications method, the secure key being stored in the mobile terminal for use during the secure communications session;

encrypting and transmitting data to the mobile terminal using a current session key, and receiving and decrypting data received from the mobile terminal using the current session key; and

ending the secure communications session by an access point (AP) in response to receiving a logoff message from the mobile terminal, the logoff message being in encrypted form and including the secure key.

8. A method for providing a secure communications session with a mobile terminal in a wireless local area network (WLAN), the method comprising the steps of:

generating a secure keys and a secure seed;

transmitting the secure keys and the secure seed to the WLAN using a secure communications method, the secure keys and the secure seed being stored in the WLAN for use during the secure communications session;

encrypting and transmitting data to the WLAN using a current session key, and receiving and decrypting data received from the WLAN using the current session key, the secure key initially being used as the current session key; and

periodically generating by the mobile terminal a subsequent session key using the secure seed and using the subsequent session key as the current session key during subsequent communications with the WLAN.

IPEA/US

9. The method as in claim 8, wherein the periodically generating step comprises generating by the mobile terminal a subsequent session key using a combination of a new key and the secure seed, the new key being generated using the secure key.

10. The method as in claim 9, wherein the periodically generating step comprises generating by the mobile terminal a subsequent session key by concatenating the new key and the secure seed and running a hash algorithm to generate the subsequent session key.

11. A method for providing a secure communications session with a mobile terminal in a wireless local area network (WLAN), the method comprising the steps of:

generating a secure key;

receiving the secure key from the WLAN using a secure communications method, the secure key being stored in the WLAN for use during the secure communications session;

encrypting and transmitting data to the WLAN using a current session key, and receiving and decrypting data received from the WLAN using the current session key; and

ending the secure communications session in response to receiving a logoff message from the WLAN, the logoff message being in encrypted form and including the secure key.

12. A method for providing a secure communications session with a mobile terminal in a wireless local area network (WLAN), the method comprising the steps of:

installing at least two shared secrets on both the mobile terminal and the WLAN access point during the user authentication phase whereby a first secret is the initial session key and a second secret is utilized as secure seed to generate subsequent session keys.

13. The method as in claim 12, further comprising the step of generating a new key and encrypting the new key with the current session key and exchanging and the new key between the WLAN and the mobile terminal.

14. The method as in claim 12, further comprising the step of the WLAN and the mobile terminal generating a new session key employing the new session key and the secure seed.

15. The method as in claim 14, wherein generating the new session key generation comprises the step of concatenating the said new session key to the secure seed.

IPEA/US

PCT/US04/07403 . 08122004

16. The method as in claim 15, further comprising the step of generating a new session key by applying a hash algorithm on said concatenated result.

17. The method as in claim 16, further comprising the step of using the said new session key in communications between the WLAN and mobile terminal.

18. A method for providing a secure communications session between a mobile terminal and a wireless local area network (WLAN), the method comprising the steps of:

a mobile terminal sending during session logoff an encrypted logoff request accompanied by the secure seed such that the secure seed appears in the logoff request.

19. An access point for providing a secure communications session between a mobile terminal and a wireless local area network (WLAN), comprising:

a means for transmitting a secure keys and a secure seed to the mobile terminal using a secure communications method;

a means to encrypt data using the secure key; and

a means to periodically generate a subsequent session key using the secure seed.

20. A terminal device for providing a secure communications session with a communications network, comprising:

a means to receive a secure key and a secure seed and a means to store the secure key and the secure seed for use during the secure communications session;

a means to receive data and a means to decrypt the data using a current session key during the secure communications session, the secure key being using initially as the current session key; and

a means to generate a subsequent session key using the current session key and the secure seed, the subsequent session key thereafter being used as the current session key for subsequent communications.

21. The terminal device according to claim 20, wherein the terminal device comprises a mobile terminal and the communications network comprises a wireless local area network (WLAN).

AMENDED SHEET

IPEA/US

PCT/US04/07403 . 08122004

22. The access point according to claim 24, wherein the means to periodically generate a subsequent session key comprises a means to generate a subsequent session key using a combination of a new key and the secure seed, the new key being generated by means using the secure key.

23. The access point according to claim 24, wherein the means to periodically generate a subsequent session key comprises a means to generate a subsequent session key by concatenating a new key and the second secure seed and a means for running a hash algorithm to generate the subsequent session key.

24. An access point (AP) for providing a secure communications session between a mobile terminal and a wireless local area network, comprising:

a means to transmit a secure key and a secure seed and a means to store the secure key and the secure seed for use during the secure communications session;

a means to encrypt data and a means to transmit data to the mobile terminal and a means to receive data and a means to decrypt the data from the mobile terminal using a current session key during the secure communications session, the secure key being using initially as the current session key; and

a means to generate a subsequent session key using the current session key and the secure seed, the subsequent session key thereafter being used as the current session key for subsequent communications.

AMENDED SHEET

IPEA/US

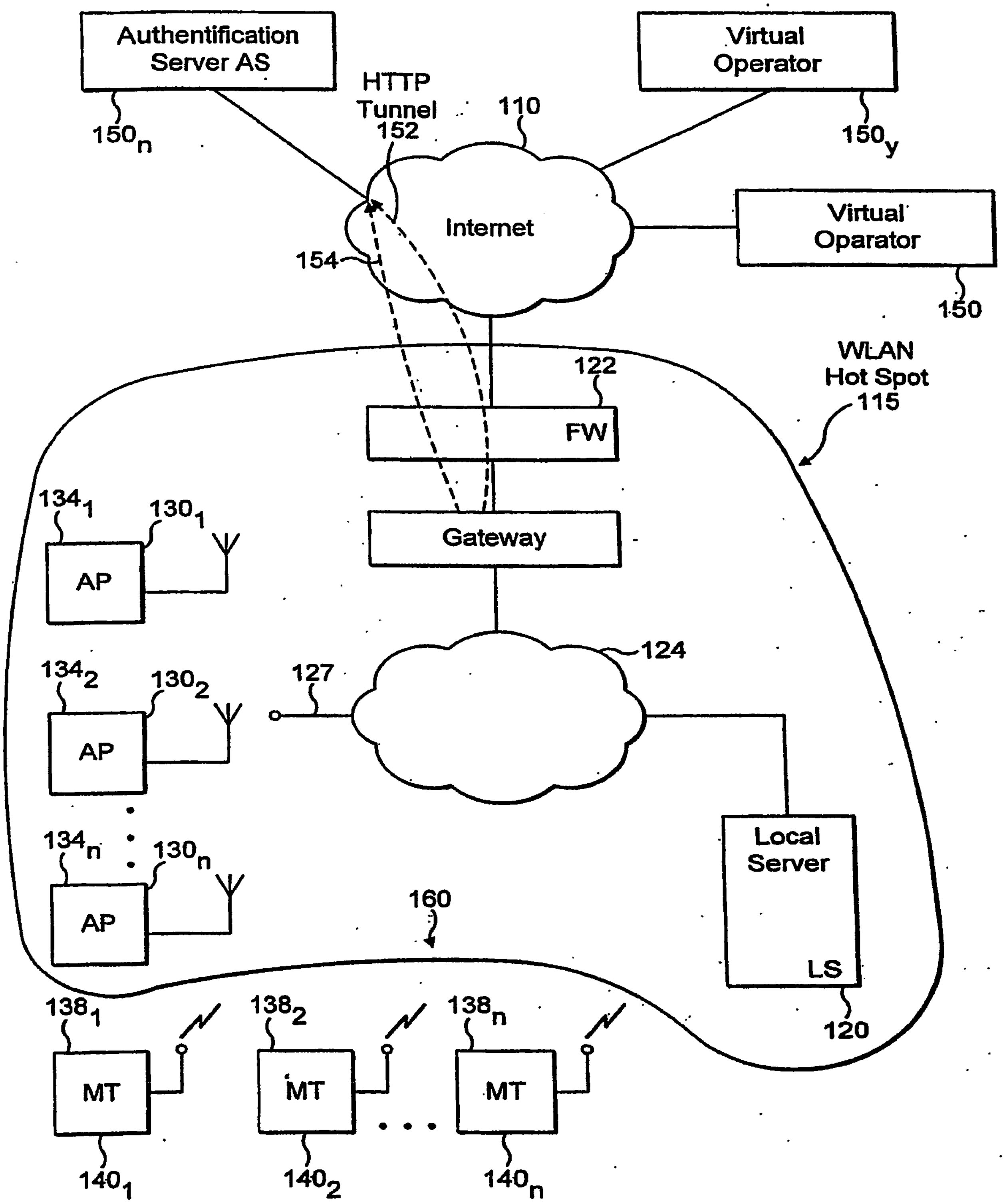

FIG. 1

AMENDED SHEET

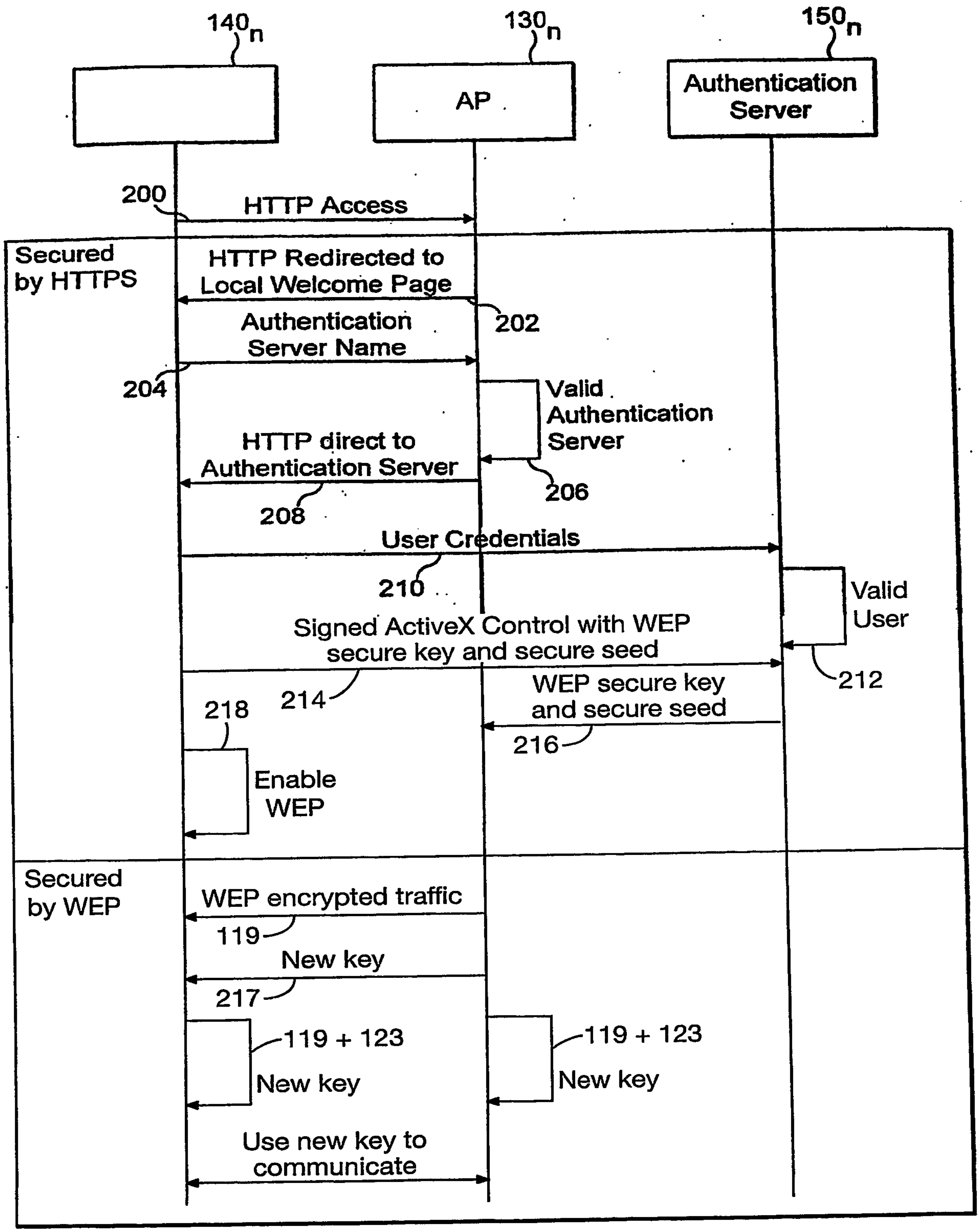
140n
130n
150n
AP
Authentication Server
200
HTTP Access
Secured by HTTPS
HTTP Redirected to Local Welcome Page
202
Authentication Server Name
204
Valid Authentication Server
206
HTTP direct to Authentication Server
208
User Credentials
210
Valid User
212
Signed ActiveX Control with WEP secure key and secure seed
214
WEP secure key and secure seed
216
218
Enable WEP
Secured by WEP
WEP encrypted traffic
119
New key
217
119 + 123
New key
119 + 123
New key
Use new key to communicate

FIG. 2

AMENDED SHEET

IPEA/US

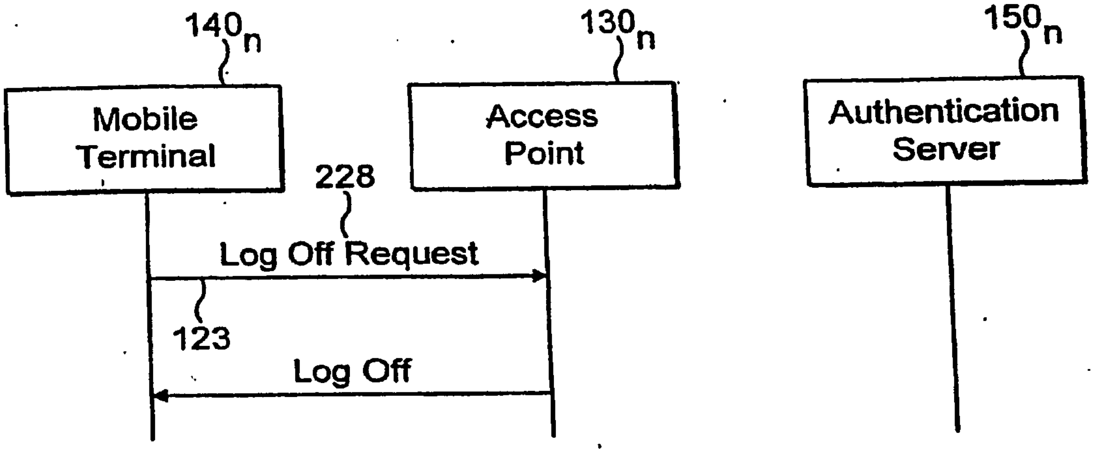

FIG. 3

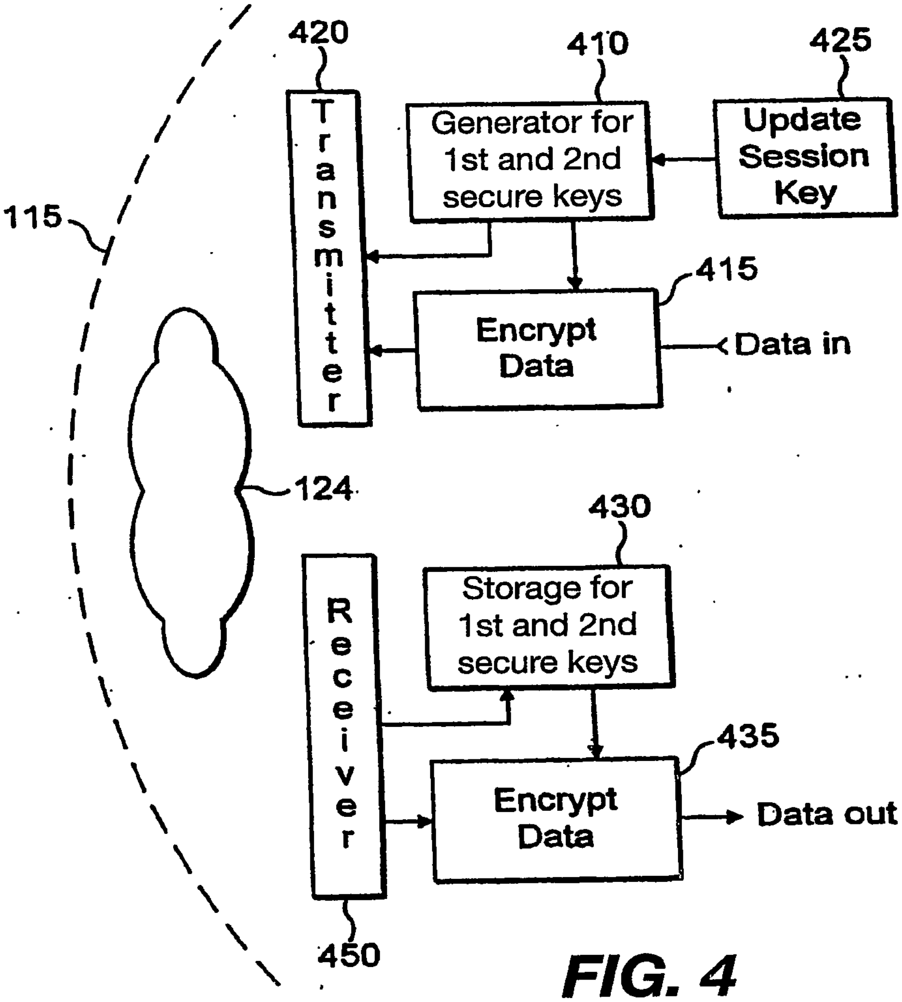

FIG. 4

AMENDED SHEET